

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)**End of Result Set**

Generate Collection

Print

L24: Entry 4 of 4

File: USPT

May 1, 2001

US-PAT-NO: 6226618

DOCUMENT-IDENTIFIER: US 6226618 B1

TITLE: Electronic content delivery system

DATE-ISSUED: May 1, 2001

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Downs; Edgar	Fort Lauderdale	FL		
Gruse; George Gregory	Lighthouse Point	FL		
Hurtado; Marco M.	Boca Raton	FL		
Lehman; Christopher T.	Delray Beach	FL		
Milsted; Kenneth Louis	Boynton Beach	FL		
Lotspiech; Jeffrey B.	San Jose	CA		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE	CODE
International Business Machines Corporation	Armonk	NY				02

APPL-NO: 09/ 133519 [PALM]

DATE FILED: August 13, 1998

## PARENT-CASE:

CROSS-REFERENCE TO RELATED APPLICATIONS This non-provisional application claims subject matter that is technically related to the following applications that are commonly assigned herewith to International Business Machines (IBM). APPLI- CATION ATTORNEY SERIAL TITLE OF THE DOC. NO. NO. INVENTION INVENTOR(S) SE9-98-006 09/152,756 Secure Electronic Kenneth L. Milsted Content George Gregory Gruse Management Marco M. Hurtado Edgar Downs Cesar Medina SE9-98-007 09/209,440 Multimedia Player George Gregory Gruse Toolkit John J. Dorak, Jr. Kenneth L. Milsted SE9-98-008 09/241,276 Multimedia Content Kenneth L. Milsted Creation System Qing Gong Edgar Downs SE9-98-009 09/177,096 System for Tracking George Gregory Gruse End-User Electronic John J. Dorak, Jr. Content Kenneth L. Milsted SE9-98-010 09/203,307 Key Management Jeffrey B. Lotspiech System for End- Marco M. Hurtado User Digital Player George Gregory Gruse Kenneth L. Milsted SE9-98-011 09/208,774 Multi-media player Marco M. Hurtado for an Electronic George Gregory Gruse Content Delivery Edgar Downs System Kenneth L. Milsted SE9-98-013 09/203,306 A method to Kenneth L. Milsted identify CD content Craig Kindell Qing Gong SE9-98-014 09/203,315 Toolkit for Richard Spagna delivering electronic Kenneth L. Milsted content from an David P. Lybrand Online store. Edgar Downs SE9-98-015 09/201,622 A method and Kenneth L. Milsted apparatus to Kha Kinh Nguyen automatically create Qing Gong encode audio SE9-98-016 A method and Kenneth L. Milsted apparatus to Qing Gong indicate an encoding rate for audio

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 705/1; 705/1, 705/26, 705/27, 705/51, 705/53, 705/57, 705/59, 705/71, 380/4, 380/23, 380/24, 380/25, 380/44, 380/279, 380/281, 380/282

US-CL-CURRENT: 705/1; 380/279, 380/281, 380/282, 380/285, 380/30, 380/44, 705/26, 705/27, 705/51, 705/53, 705/57, 705/59, 705/71

FIELD-OF-SEARCH: 705/4, 705/51, 705/53, 705/57, 705/59, 705/71, 705/26, 705/27, 380/4, 380/44, 380/23, 380/25, 380/281, 380/282, 380/279, 707/9

PRIOR-ART-DISCLOSED:

## U.S. PATENT DOCUMENTS

Search Selected

Search ALL

Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/>	<u>4200770</u>	April 1980	Hellman et al.	
<input type="checkbox"/>	<u>4218582</u>	August 1980	Hellman et al.	
<input type="checkbox"/>	<u>4272810</u>	June 1981	Gates et al.	
<input type="checkbox"/>	<u>4405829</u>	September 1983	Rivest et al.	
<input type="checkbox"/>	<u>4424414</u>	January 1984	Hellman et al.	
<input type="checkbox"/>	<u>4463387</u>	July 1984	Hashimoto et al.	
<input type="checkbox"/>	<u>4528643</u>	July 1985	Freeny, Jr.	
<input type="checkbox"/>	<u>4731840</u>	March 1988	Mniszewski et al.	
<input type="checkbox"/>	<u>4757534</u>	July 1988	Matyas et al.	
<input type="checkbox"/>	<u>4782529</u>	November 1988	Shima	
<input type="checkbox"/>	<u>4803725</u>	February 1989	Horne et al.	
<input type="checkbox"/>	<u>4809327</u>	February 1989	Shima	
<input type="checkbox"/>	<u>4825306</u>	April 1989	Robers	
<input type="checkbox"/>	<u>4868687</u>	September 1989	Penn et al.	
<input type="checkbox"/>	<u>4868877</u>	September 1989	Fischer	
<input type="checkbox"/>	<u>4878246</u>	October 1989	Pastor et al.	
<input type="checkbox"/>	<u>4879747</u>	November 1989	Leighton et al.	
<input type="checkbox"/>	<u>4905163</u>	February 1990	Garber et al.	
<input type="checkbox"/>	<u>4926479</u>	May 1990	Goldwasser et al.	
<input type="checkbox"/>	<u>4944006</u>	July 1990	Citta et al.	
<input type="checkbox"/>	<u>4995082</u>	February 1991	Schnorr	
<input type="checkbox"/>	<u>5005200</u>	April 1991	Fischer	
<input type="checkbox"/>	<u>5130792</u>	July 1992	Tindell et al.	
<input type="checkbox"/>	<u>5159634</u>	October 1992	Reeds, III	
<input type="checkbox"/>	<u>5191573</u>	March 1993	Hair	

<input type="checkbox"/>	<u>5214702</u>	May 1993	Fischer	
<input type="checkbox"/>	<u>5220604</u>	June 1993	Gasser et al.	
<input type="checkbox"/>	<u>5224163</u>	June 1993	Gasser et al.	
<input type="checkbox"/>	<u>5224166</u>	June 1993	Hartman, Jr.	
<input type="checkbox"/>	<u>5260788</u>	November 1993	Takano et al.	
<input type="checkbox"/>	<u>5261002</u>	November 1993	Perlman et al.	
<input type="checkbox"/>	<u>5276901</u>	January 1994	Howell et al.	
<input type="checkbox"/>	<u>5315658</u>	May 1994	Micali	
<input type="checkbox"/>	<u>5319705</u>	June 1994	Halter et al.	
<input type="checkbox"/>	<u>5347580</u>	September 1994	Molva et al.	
<input type="checkbox"/>	<u>5355302</u>	October 1994	Martin et al.	
<input type="checkbox"/>	<u>5369705</u>	November 1994	Bird et al.	
<input type="checkbox"/>	<u>5371794</u>	December 1994	Diffie et al.	
<input type="checkbox"/>	<u>5412717</u>	May 1995	Fischer	
<input type="checkbox"/>	<u>5420927</u>	May 1995	Micali	
<input type="checkbox"/>	<u>5497421</u>	March 1996	Kaufman et al.	
<input type="checkbox"/>	<u>5509071</u>	April 1996	Petrie, Jr. et al.	
<input type="checkbox"/>	<u>5519778</u>	May 1996	Leighton et al.	
<input type="checkbox"/>	<u>5537475</u>	July 1996	Micali	
<input type="checkbox"/>	<u>5557541</u>	September 1996	Schulhof et al.	
<input type="checkbox"/>	<u>5581479</u>	December 1996	McLaughlin et al.	
<input type="checkbox"/>	<u>5588060</u>	December 1996	Aziz	
<input type="checkbox"/>	<u>5592664</u>	January 1997	Starkey	
<input type="checkbox"/>	<u>5604804</u>	February 1997	Micali	
<input type="checkbox"/>	<u>5606617</u>	February 1997	Brands	
<input type="checkbox"/>	<u>5636139</u>	June 1997	McLaughlin et al.	
<input type="checkbox"/>	<u>5646992</u>	July 1997	Subler et al.	
<input type="checkbox"/>	<u>5646998</u>	July 1997	Stambler	
<input type="checkbox"/>	<u>5666420</u>	September 1997	Micali	
<input type="checkbox"/>	<u>5673316</u>	September 1997	Auerbach et al.	
<input type="checkbox"/>	<u>5675734</u>	October 1997	Hair	
<input type="checkbox"/>	<u>5706347</u>	January 1998	Burke et al.	705/71
<input type="checkbox"/>	<u>5710887</u>	January 1998	Chelliah et al.	
<input type="checkbox"/>	<u>5745574</u>	April 1998	Muftic	
<input type="checkbox"/>	<u>5765152</u>	June 1998	Erickson	707/9
<input type="checkbox"/>	<u>5796841</u>	August 1998	Cordery et al.	
<input type="checkbox"/>	<u>5864620</u>	January 1999	Pettitt	380/4
	<u>5889860</u>	March 1999	Eller et al.	705/51

<input type="checkbox"/>				
<input type="checkbox"/>	<u>5892900</u>	April 1999	Ginter et al.	
<input type="checkbox"/>	<u>5915025</u>	December 1999	Taguchi et al.	380/44
<input type="checkbox"/>	<u>5982892</u>	November 1999	Hicks et al.	705/71
<input type="checkbox"/>	<u>5991399</u>	November 1999	Graunke et al.	380/279
<input type="checkbox"/>	<u>5999629</u>	December 1999	Heer et al.	705/51

## OTHER PUBLICATIONS

J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, Feb., 1993, pp. 1-37.  
S. Kent, "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management". RFC 1422, Feb., 1993, pp. 1-28.  
D. Balenson, "Privacy Enhancement for Internet Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, Feb. 1993, pp. 1-13.  
B. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, Feb. 1993, pp. 1-8.

ART-UNIT: 274

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Nguyen; Nga B.

ATTY-AGENT-FIRM: Meyers; Steven J. Soucar; Steven J. Fleit, Kain, Gibbons, Gutman &amp; Bongini P.L.

## ABSTRACT:

Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system, the method comprising the steps of: transferring the encrypted data decrypting key to a clearing house that possesses a first private key, which corresponds to the first public key; decrypting the data decrypting key using the first private key; re-encrypting the data decrypting key using a second public key; transferring the re-encrypted data decrypting key to the user's system, the user's system possessing a second private key, which corresponds to the second public key; and decrypting the re-encrypted data decrypting key using the second private key.

26 Claims, 20 Drawing figures

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)**End of Result Set**

Generate Collection

Print

L24: Entry 4 of 4

File: USPT

May 1, 2001

DOCUMENT-IDENTIFIER: US 6226618 B1

TITLE: Electronic content delivery system

Application Filing Date (1):19980813Detailed Description Text (146):

Either a Key Identifier to indicate the public encryption key that was used to encrypt the part of an encrypted symmetric key that, when decrypted, is used to decrypt the encrypted part.

Detailed Description Text (175):

Watermarking Instructions--A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the License SC(s) 660. There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions, the output part name to use when the watermarking instructions are decrypted, a base64 encoding of the encrypted Symmetric Key 623 bitstring that is was used to encrypt the watermarking instructions, the encryption algorithm that was used to encrypt the Symmetric Key 623, and the identification of the public key that is required to decrypt the Symmetric Key 623.

Current US Original Classification (1):705/1Current US Cross Reference Classification (9):705/51Current US Cross Reference Classification (11):705/57Current US Cross Reference Classification (12):705/59[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)**End of Result Set**

Generate Collection

Print

L27: Entry 1 of 1

File: USPT

Jan 8, 2002

DOCUMENT-IDENTIFIER: US 6337912 B1

TITLE: Method of and system for writing-in key information

Application Filing Date (1):19970819

## CLAIMS:

5. A system for securely transforming a data carrier remotely into a key associated with a particular object identified by object information, comprising;

a data carrier having a data carrier memory for storing secret identification information of said data carrier that is not externally accessible and for also storing open further identification information of said data carrier that is externally accessible;

a central station having a central station memory for storing said secret identification information in association with said open identification information and for storing said object information and key information in association with said object information;

a remote station for retrieving said further identification information from said data carrier memory and for entering said object information;

said remote station including a first encryption section for encrypting said entered object information with said retrieved further identification information to produce first encrypted object information, and a second encryption section using an asymmetrical encryption/decryption process having a public encryption key stored at said remote station and a corresponding secret description key stored at said central station for further encrypting said first encrypted object information to produce second encrypted object information;

said remote station transmitting and said central station receiving said second encrypted object information and said retrieved further identification information;

said central station further including a first decryption section for decrypting said received second encrypted object information with said stored secret decryption key to recreate said first encrypted object information and a second decryption section for further decrypting said recreated first encrypted object information with said received further identification information to recreate said object information;

said central station retrieving said secret identification information associated with said further identification information and retrieving said key information associated with said recreated object information;

said central station further including an encryption section for encrypting said

retrieved key information with said retrieved secret identification information, said central station transmitting and said remote station receiving said encrypted key information;

said remote station retrieving said stored secret identification information and including a decryption section for decrypting said received encrypted key information with said retrieved secret identification information to recreate said key information; and

said remote station storing said recreated key information in said data carrier to transform said data carrier into said key associated with said particular object.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

## Refine Search

Your wildcard search against 10000 terms has yielded the results below.

***Your result set for the last L# is incomplete.***

The probable cause is use of unlimited truncation. Revise your search strategy to use limited truncation.

### Search Results -

Terms	Documents
(encrypt\$ with decrypt\$ with public\$ with key\$) and @ad<=19990327	1

**Database:**

US Pre-Grant Publication Full-Text Database  
 US Patents Full-Text Database  
 US OCR Full-Text Database  
 EPO Abstracts Database  
 JPO Abstracts Database  
 Derwent World Patents Index  
 IBM Technical Disclosure Bulletins

**Search:**

L27

Refine Search

Recall Text

Clear

Interrupt

### Search History

**DATE:** Monday, September 12, 2005    [Printable Copy](#)    [Create Case](#)

<u>Set</u> <u>Name</u> side by side	<u>Query</u>	<u>Hit</u> <u>Count</u>	<u>Set</u> <u>Name</u> result set
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
<u>L27</u>	(encrypt\$ with decrypt\$ with public\$ with key\$) and @ad<=19990327	1	<u>L27</u>
<u>L26</u>	(encrypt\$ with decrypt\$ with public\$ with key\$) and L24	0	<u>L26</u>
<u>L25</u>	(ecrypt\$ with decrypt\$ with public\$ with key\$) and L24	0	<u>L25</u>
<u>L24</u>	L23 and @ad<=19990327	4	<u>L24</u>
<u>L23</u>	L22 and l19	14	<u>L23</u>
<u>L22</u>	705/50,51,57-59.ccls.	2103	<u>L22</u>
<u>L21</u>	L20 and @ad<=19990327	9	<u>L21</u>
<u>L20</u>	L19 and (key adj2 identif\$)	24	<u>L20</u>
<u>L19</u>	L17 and ((key\$ near4 identif\$) with decrypt\$)	34	<u>L19</u>
<u>L18</u>	L17 and (key\$ near4 identif\$)	914	<u>L18</u>



<u>L17</u>	705/?ccls.	10489	<u>L17</u>
<u>L16</u>	L15 and accelerat\$	2	<u>L16</u>
<u>L15</u>	L1 and (((road or surface) with (coef\$ or friction)) and (chang\$ with speed with (connect\$ or disconnect\$)))	3	<u>L15</u>
<u>L14</u>	L1 and (((road or surface) with (coef\$ or friction)) same (chang\$ with speed with (connect\$ or disconnect\$)))	0	<u>L14</u>
<u>L13</u>	L2 and (((road or surface) with (coef\$ or friction)) same (chang\$ with speed with (connect\$ or disconnect\$)))	0	<u>L13</u>
<i>DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR</i>			
<u>L12</u>	L10 and DNsr	1	<u>L12</u>
<u>L11</u>	L10 and (chang\$ with speed with (connect\$ or disconnect\$))	1	<u>L11</u>
<u>L10</u>	6898504.pn.	1	<u>L10</u>
<i>DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR</i>			
<u>L9</u>	L8 and (chang\$ with speed with (connect\$ or disconnect\$))	1	<u>L9</u>
<u>L8</u>	L7 and ((road or surface) with coefficient)	7	<u>L8</u>
<u>L7</u>	L2 and ((road or surface) with friction)	32	<u>L7</u>
<i>DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR</i>			
<u>L6</u>	L4 and (chang\$ with speed with connect\$ with disconnect\$)	1	<u>L6</u>
<u>L5</u>	L4 and (chang\$ with speed)	45	<u>L5</u>
<u>L4</u>	L3 and (shaft with power\$)	65	<u>L4</u>
<u>L3</u>	L2 and (shaft with transmission)	143	<u>L3</u>
<u>L2</u>	L1 and (clutch with control\$)	187	<u>L2</u>
<u>L1</u>	701/67.ccls. and clutch and vehicle	191	<u>L1</u>

END OF SEARCH HISTORY

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

End of Result Set

☐ [Generate Collection](#) [Print](#)

No license

L27: Entry 1 of 1

File: USPT

Jan 8, 2002

US-PAT-NO: 6337912

DOCUMENT-IDENTIFIER: US 6337912 B1

TITLE: Method of and system for writing-in key information

DATE-ISSUED: January 8, 2002

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Buhr; Wolfgang	Hamburg			DE
Horner; Helmut	Hamburg			DE

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
U.S. Philips Corporation	New York	NY			02

APPL-NO: 08/ 914444 [\[PALM\]](#)

DATE FILED: August 19, 1997

## FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
DE	196 33 802	August 22, 1996

INT-CL: [07] [H04 L 9/12](#), [H04 L 9/00](#), [H04 K 1/00](#)

US-CL-ISSUED: 380/279; 380/260, 713/185

US-CL-CURRENT: [380/279](#); [380/260](#), [713/185](#)

FIELD-OF-SEARCH: 380/21, 380/185, 380/259, 380/260, 380/277, 380/278, 380/279, 235/380, 235/492, 213/65, 713/185, 713/65

## PRIOR-ART-DISCLOSED:

## U.S. PATENT DOCUMENTS

[Search Selected](#)[Search ALL](#)[Clear](#)

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/> <a href="#">4926665</a>	May 1990	Stapley et al.	70/277
<input type="checkbox"/> <a href="#">5218638</a>	June 1993	Matsumoto et al.	380/23
<input type="checkbox"/> <a href="#">5623637</a>	April 1997	Jones et al.	395/491

<input type="checkbox"/>	<u>5745571</u>	April 1998	Zuk	380/21
<input type="checkbox"/>	<u>5838251</u>	November 1998	Brinkmeyer et al.	340/825.31
<input type="checkbox"/>	<u>5959276</u>	September 1999	Iijima	235/380

ART-UNIT: 2131

PRIMARY-EXAMINER: Hayes; Gail

ASSISTANT-EXAMINER: DiLorenzo; Anthony

ATTY-AGENT-FIRM: Mak; Theo

ABSTRACT:

In order to unambiguously allocate a data carrier to an object, key information is written into the data carrier. Before writing-in the key information, secret identification information and open identification information is written into the data carrier. Copies of the secret and open information are stored in a central station. In the central station, for a particular data carrier, the open and secret information is associated with each other. In addition thereto, in the central station, object information for the particular object, and key information for the object are associated with each other. From the data carrier, the open identification information is sent to the central station to access the associated stored open and secret identification information so as to retrieve the stored secret identification information. In addition thereto, object information is sent to the central station to access the associated stored object and key information so as to retrieve the stored key information. The retrieved key information is encrypted with the retrieved secret identification information and the encrypted key information is sent to the data carrier. In the data carrier, the received encrypted key information is decrypted. The decrypted key information is written into the data carrier.

8 Claims, 1 Drawing figures

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)**End of Result Set**

Generate Collection

Print

L27: Entry 1 of 1

File: USPT

Jan 8, 2002

DOCUMENT-IDENTIFIER: US 6337912 B1

TITLE: Method of and system for writing-in key information

Application Filing Date (1):19970819

## CLAIMS:

5. A system for securely transforming a data carrier remotely into a key associated with a particular object identified by object information, comprising;

a data carrier having a data carrier memory for storing secret identification information of said data carrier that is not externally accessible and for also storing open further identification information of said data carrier that is externally accessible;

a central station having a central station memory for storing said secret identification information in association with said open identification information and for storing said object information and key information in association with said object information;

a remote station for retrieving said further identification information from said data carrier memory and for entering said object information;

said remote station including a first encryption section for encrypting said entered object information with said retrieved further identification information to produce first encrypted object information, and a second encryption section using an asymmetrical encryption/decryption process having a public encryption key stored at said remote station and a corresponding secret decryption key stored at said central station for further encrypting said first encrypted object information to produce second encrypted object information;

said remote station transmitting and said central station receiving said second encrypted object information and said retrieved further identification information;

said central station further including a first decryption section for decrypting said received second encrypted object information with said stored secret decryption key to recreate said first encrypted object information and a second decryption section for further decrypting said recreated first encrypted object information with said received further identification information to recreate said object information;

said central station retrieving said secret identification information associated with said further identification information and retrieving said key information associated with said recreated object information;

said central station further including an encryption section for encrypting said

retrieved key information with said retrieved secret identification information, said central station transmitting and said remote station receiving said encrypted key information;

said remote station retrieving said stored secret identification information and including a decryption section for decrypting said received encrypted key information with said retrieved secret identification information to recreate said key information; and

said remote station storing said recreated key information in said data carrier to transform said data carrier into said key associated with said particular object.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#)[Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L24: Entry 1 of 4

File: USPT

Jan 27, 2004

DOCUMENT-IDENTIFIER: US 6684198 B1

TITLE: Program data distribution via open network

Application Filing Date (1):19970903Current US Original Classification (1):705/50Current US Cross Reference Classification (1):705/1Current US Cross Reference Classification (2):705/51Current US Cross Reference Classification (3):705/58Current US Cross Reference Classification (4):705/59

## CLAIMS:

2. A program data distribution method for use with an open network comprising the steps of: issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; distributing program data encrypted by the encryption key from a file server connected to said open network; distributing a decryption key from a key server connected to said open network, said decryption key used to decode said encrypted program data; and employing said decryption key distributed by said key server to decode said encrypted program data obtained from said file server by a terminal, which is connected to said open network for processing program data, wherein, at the step of distributing encrypted program data, the identification code is transmitted along with the program data to the terminal, the terminal transmits the received identification code to the key server, and based on the identification code, the key server searches for a decryption key used to decrypt the program data and transmits the decryption key to the terminal.

8. A program data distribution method, for use with an open network, comprising the steps of; issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; distributing program data encrypted by the encryption key from a file server connected to said open network; downloading said encrypted program data, which is distributed by said file server, at a terminal that is connected to said open network and processes said program data; distributing a decryption key from a key server connected to said open network, said decryption key used to decode said encrypted program data that is transmitted by said file server; and employing, at said terminal, said decryption key received from said key server to decode said

encrypted program data that is downloaded, wherein at the step of distributing encrypted program data the identification code is distributed along with the program data, at the step of downloading the identification code is transmitted to the key server, and at the step of distributing a decryption key the identification code is employed by the key server to search for a decryption key that is used to decode the program data.

16. A program data distribution system for use with an open network comprising: a manager for issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; a file server, connected to said open network and holding distribution rights for the program data based on a contract with said manager, for encrypting program data by the encryption key issued from the manager and distributing the encrypted program data along with the corresponding identification code; a key server, connected to said open network, and independent from the file server, for distributing the decryption key issued by said manager; and a terminal, connected to said open network, for receiving the encrypted program data along with the corresponding identification code from the file server, and obtaining the decryption key corresponding to the identification code from the key server to decode and process the encrypted program data.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L24: Entry 1 of 4

File: USPT

Jan 27, 2004

US-PAT-NO: 6684198

DOCUMENT-IDENTIFIER: US 6684198 B1

TITLE: Program data distribution via open network

DATE-ISSUED: January 27, 2004

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Shimizu; Yusuke	Tokyo			JP
Uchida; Yoichi	Tokyo			JP
Adachi; Seiiji	Tokyo			JP
Hammond; Eric Rayburn	Menlo Park	CA		
Noguchi; Yasuhiro	Emeryville	CA		
Heilman, III; Paul Mitchell	San Mateo	CA		
Poling, Jr.; Daniel Luke	Redwood City	CA		

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sega Enterprises, Ltd.				JP	03

APPL-NO: 08/ 922339 [\[PALM\]](#)

DATE FILED: September 3, 1997

INT-CL: [07] [G06 F 17/60](#)

US-CL-ISSUED: 705/50; 705/51, 705/1, 705/58, 705/59

US-CL-CURRENT: [705/50](#); [705/1](#), [705/51](#), [705/58](#), [705/59](#)

FIELD-OF-SEARCH: 705/35, 705/44, 705/1, 705/50, 705/51, 705/53, 705/54, 705/57, 705/59, 705/52, 705/64, 705/26, 380/4, 380/25, 380/21, 380/23, 713/155, 713/200

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected

Search ALL

Clear

PAT-NO

ISSUE-DATE

PATENTEE-NAME

US-CL

[4771458](#)

September 1988

Citta et al.

380/20

[5138712](#)

August 1992

Corbin

713/200

[5191611](#)

March 1993

Lang

380/25



<input type="checkbox"/>	<u>5237611</u>	August 1993	Rasmussen et al.	380/21
<input type="checkbox"/>	<u>5237614</u>	August 1993	Weiss	380/23
<input type="checkbox"/>	<u>5495533</u>	February 1996	Lineham et al.	713/155
<input type="checkbox"/>	<u>5666411</u>	September 1997	McCarty	380/4
<input type="checkbox"/>	<u>5715403</u>	February 1998	Stefik	705/44
<input type="checkbox"/>	<u>5765152</u>	June 1998	Erickson	707/9
<input type="checkbox"/>	<u>5870474</u>	February 1999	Wasilewski et al.	380/21
<input type="checkbox"/>	<u>5892900</u>	April 1999	Ginter et al.	395/186
<input type="checkbox"/>	<u>5909638</u>	June 1999	Allen	455/6.1
<input type="checkbox"/>	<u>6000030</u>	December 1999	Steinberg et al.	713/200
<input type="checkbox"/>	<u>6135646</u>	October 2000	Kahn et al.	395/200.47

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
05081204	April 1993	JP	

## OTHER PUBLICATIONS

Denning, Dorothy E.; Branstad, Dennis K., "A taxonomy for key escrow encryption systems", Communications of the ACM v39n3 PP:34-39 Mar. 1996.

ART-UNIT: 3621

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Hewitt; Calvin

ATTY-AGENT-FIRM: Dickstein Shapiro Morin & Oshinsky LLP

## ABSTRACT:

When program data is distributed to users across an open network, such as the Internet, a licensing agreement concluded between a server for the program data and a manager is maintained and the unauthorized copying of program data is prevented. Therefore, to fulfill such the situation, a program data distribution system includes an open network; a file server, connected to the open network, for distributing encrypted program data; a key server, connected to the open network, for distributing a decryption key used to decode the encrypted program data; and a terminal, connected to the open network, for processing program data, the terminal employing the decryption key distributed by the key server to decode the encrypted program data obtained from the file server.

22 Claims, 4 Drawing figures

[Previous Doc](#)   [Next Doc](#)   [Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L24: Entry 2 of 4

File: USPT

Mar 25, 2003

DOCUMENT-IDENTIFIER: US 6539364 B2

TITLE: Electronic cash implementing method and equipment using user signature and recording medium recorded thereon a program for the method

Application Filing Date (1):19981223Detailed Description Text (138):

The issuer equipment 100 retrieves the common key K corresponding to the identification number KID from the storage device 110, extracts the key PKUi, the identification number KID and the amount x by decryption with the common key K, and increments the balance counter EBC by x. Further, the issuer equipment 100 attaches its signature to a pair of the key PKUi and the amount x using the issuer secret key SKI to obtain SKI(PKUi, x), then encrypts it with the common key K to obtain K(SKI(PKUi, x)), and sends it intact (in FIG. 20) to the bank 200 or together with the issuer signature generated using the secret key SKI (in FIG. 24).

Current US Cross Reference Classification (1):705/1Current US Cross Reference Classification (2):705/50

## CLAIMS:

11. The method of claim 1 or 2, wherein said electronic cash system further comprises a bank equipment as an institution for managing an account of each user, and said method comprises: user registration procedure wherein: said user equipment generates a common key, then encrypts a signature verifying public key and said common key as a pseudonym of said user with an issuer public key, and sends said encrypted pseudonym to said bank equipment together with user identification information IdU; said bank equipment stores said user identification information IdU and said encrypted pseudonym, and sends said encrypted pseudonym to said issuer equipment; said issuer equipment decrypts said encrypted data from said bank equipment with an issuer secret key to extracts said pseudonym and said common key, then adds an identifier for said common key as common key information KID, then stores said pseudonym and said encrypted pseudonym, and at the same time, stores said common key information KID and said common key in correspondence with each other, then generates an issuer signature for said pseudonym as a license, then encrypts said license and said common key information KID with said common key to obtain an encrypted license, and sends said encrypted license to said bank equipment; and said bank equipment sends said encrypted information received from said issuer equipment to said user equipment; and said user equipment decrypts said encrypted license with said common key to extract said license and said common key information KID, and stores them; electronic cash issuing procedure wherein: said user equipment encrypts its pseudonym and its requested amount of withdrawal with said common key to obtain an encrypted pseudonym, and sends said common key information KID and said encrypted pseudonym to said bank equipment together with user identification information IdU and said requested amount; said bank equipment reduces the balance in an account of said user in response to said request from

said user equipment, and sends to said issuer equipment said requested amount, said encrypted pseudonym and said common key information KID received from said user equipment; said issuer equipment retrieves said common key corresponding to said common key information KID received from said bank equipment, decrypts said received encrypted pseudonym with said common key to extract said user pseudonym, then generates as electronic cash an issuer signature for said user pseudonym and said requested amount, then encrypts said electronic cash with said common key, then increments said electronic cash balance counter corresponding to said user pseudonym by the amount of said encrypted electronic cash, and sends said encrypted electronic cash to said bank equipment; said bank equipment sends said encrypted electronic cash to said user equipment; and said user equipment decrypts said encrypted electronic cash with said common key, verifies the validity of said issuer signature of said electronic cash, and if valid, increments said user balance counter by the amount of said electronic cash received from said bank equipment without storing the electronic cash; and electronic cash payment procedure wherein: said user equipment decrements said balance counter by the amount due, generates a user signature therefor, and sends said user signature to said shop equipment together with said license and said user pseudonym.

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L24: Entry 2 of 4

File: USPT

Mar 25, 2003

US-PAT-NO: 6539364

DOCUMENT-IDENTIFIER: US 6539364 B2

TITLE: Electronic cash implementing method and equipment using user signature and recording medium recorded thereon a program for the method

DATE-ISSUED: March 25, 2003

## INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Moribatake; Hidemi	Tokyo			JP
Okamoto; Tatsuaki	Tokyo			JP

## ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE	CODE
Nippon Telegraph and Telephone Corporation	Tokyo			JP		.03

APPL-NO: 09/ 219447 [\[PALM\]](#)

DATE FILED: December 23, 1998

## FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-359106	December 26, 1997

INT-CL: [07] [G06](#) [F](#) [17/60](#)

US-CL-ISSUED: 705/69; 705/1, 705/50, 705/64, 705/65, 705/66, 705/67, 705/68, 705/76, 705/78

US-CL-CURRENT: [705/69](#); [705/1](#), [705/50](#), [705/64](#), [705/65](#), [705/66](#), [705/67](#), [705/68](#), [705/76](#), [705/78](#)

FIELD-OF-SEARCH: 705/1, 705/78, 705/35, 705/39, 705/41, 705/50, 705/53, 705/64, 705/65, 705/76, 705/75, 380/4, 380/23, 380/24, 380/25, 380/30, 380/21

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected

Search ALL

Clear

PAT-NO

ISSUE-DATE

PATENTEE-NAME

US-CL

[5536923](#)

July 1996

Foglino

235/380

[5696827](#)

December 1997

Brands

380/30

<input type="checkbox"/>	<u>5889862</u>	March 1999	Ohta et al.	380/24
<input type="checkbox"/>	<u>5901229</u>	May 1999	Fujisaki et al.	380/30
<input type="checkbox"/>	<u>5926548</u>	July 1999	Okamoto	380/24
<input type="checkbox"/>	<u>6164528</u>	December 2000	Hills et al.	235/379
<input type="checkbox"/>	<u>6209095</u>	March 2001	Anderson et al.	713/176

## FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 772 165	May 1997	EP	
0 807 910	November 1997	EP	
0 810 563	December 1997	EP	
0 810 563	January 2000	EP	
03-073065	March 1991	JP	
03-092966	April 1991	JP	
09006880	January 1997	JP	
WO 97 08870	March 1997	WO	

## OTHER PUBLICATIONS

Tyler, Geoff, "The cashless revolution", Management Services, v39n6 pp: 26-27 Jun. 1995.\*

Hidemi Moribatake et al., SCIS97-3C (Symposium on Cryptography and Information Security), 1997, pp. 1-8, Electronic Cash Scheme.

XP 000567597; Electronic Cash on the Internet by Stefan Brands.

Brands, S., "Off-Line Cash transfer by Smart Cards," Centrum Voor Wiskunde en Informatica Report, No. CS-R9455, Jan. 1, 1994, pp. 1-16.

Camenisch, J., et al., "An Efficient Fair Payment System," 3rd ACM Conf. on Computer and Communications Security, New Delhi, Mar. 14-16, 1996, No. Conf. 3, Mar. 14, 1996, pp. 88-94.

New Electronic Money System NTT Review, vol. 8, No. 6, Nov. 1, 1996, p. 4.

Zuzuki, M., et al., "Electronic Cash System," NTT Review, vol. 8, No. 4, Jul. 1, 1996, pp. 10-15..

ART-UNIT: 3621

PRIMARY-EXAMINER: Sough; Hyung-Sub

ASSISTANT-EXAMINER: Hewitt, II; Calvin L

ATTY-AGENT-FIRM: Connolly Bove Lodge & Hutz LLP

## ABSTRACT:

A user registers a user public key PKU as a pseudonym at a trustee or issuer and obtains an signature for the pseudonym as a license. The sends the pseudonym, PKU identification information IdU and the amount of withdrawal x to the issuer institution. The issuer increments a balance counter of the pseudonym by x, then generates an issuer signature SKI(PKU, x) with a secret key SKI, and sends the issuer signature as an electronic cash to the user. The user verifies the validity of the issuer signature with a public key SKI, and if valid, increments an electronic cash balance counter Balance by x. At the time of payment, user sends

the public key PKU and the license to a shop, and the shop verifies the validity of the license, and if valid, sends a challenge to the user. The user attaches a signature to the challenge with user secret key SKU, then sends it to the shop together with the amount due  $y$ , and decrements the electronic cash balance counter by  $y$ .

25 Claims, 30 Drawing figures

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L24: Entry 3 of 4

File: USPT

Sep 11, 2001

DOCUMENT-IDENTIFIER: US 6289314 B1

TITLE: Pay information providing system for descrambling information from plural sources and rescrumbling the information before sending to a terminal or terminals

Application Filing Date (1):

19970916

Detailed Description Text (25):

The terminal information setting portion 251 assigns the terminal encryption key and the coefficient of basic charge for the terminal 3 which generated the initialization command, and then stores in the terminal information storing portion 252 the identifier and the terminal information of the terminal 3 which are included in the initialization command and the assigned coefficient of basic charge and terminal encryption key (refer to FIG. 4 and FIG. 5). As described above, the terminal information setting portion 251 generates a terminal decryption key corresponding to the assigned terminal encryption key, and then generates and outputs a key assignment command to the server I/F 24. The key assignment command includes the identifier of the terminal 3 which generated the above initialization command and the terminal decryption key generated for the terminal 3, being outputted to the local bus 5 by the server I/F 24 and being inputted to the terminal I/F 32 of the terminal 3 which generated the above initialization command. The terminal I/F 32 outputs the inputted key assignment command to the terminal decrypting portion 34. The terminal decrypting portion 34 extracts the terminal decryption key included in the inputted key assignment command, and then stores the extracted terminal decryption key in its internal memory. The initialization is thereby completed, allowing the terminal 3 to generate a request for pay information.

Current US Original Classification (1):

705/1

Current US Cross Reference Classification (3):

705/50

Current US Cross Reference Classification (4):

705/51

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)



L24: Entry 1 of 4

File: USPT

Jan 27, 2004

DOCUMENT-IDENTIFIER: US 6684198 B1

TITLE: Program data distribution via open network

Application Filing Date (1):19970903Current US Original Classification (1):705/50Current US Cross Reference Classification (1):705/1Current US Cross Reference Classification (2):705/51Current US Cross Reference Classification (3):705/58Current US Cross Reference Classification (4):705/59

## CLAIMS:

2. A program data distribution method for use with an open network comprising the steps of: issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; distributing program data encrypted by the encryption key from a file server connected to said open network; distributing a decryption key from a key server connected to said open network, said decryption key used to decode said encrypted program data; and employing said decryption key distributed by said key server to decode said encrypted program data obtained from said file server by a terminal, which is connected to said open network for processing program data, wherein, at the step of distributing encrypted program data, the identification code is transmitted along with the program data to the terminal, the terminal transmits the received identification code to the key server, and based on the identification code, the key server searches for a decryption key used to decrypt the program data and transmits the decryption key to the terminal.

8. A program data distribution method, for use with an open network, comprising the steps of; issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; distributing program data encrypted by the encryption key from a file server connected to said open network; downloading said encrypted program data, which is distributed by said file server, at a terminal that is connected to said open network and processes said program data; distributing a decryption key from a key server connected to said open network, said decryption key used to decode said encrypted program data that is transmitted by said file server; and employing, at said terminal, said decryption key received from said key server to decode said



encrypted program data that is downloaded, wherein at the step of distributing encrypted program data the identification code is distributed along with the program data, at the step of downloading the identification code is transmitted to the key server, and at the step of distributing a decryption key the identification code is employed by the key server to search for a decryption key that is used to decode the program data.

16. A program data distribution system for use with an open network comprising: a manager for issuing an identification code corresponding to program data, an encryption key which is used to encrypt said program data and a decryption key which is used to decode the program data encrypted by the encryption key; a file server, connected to said open network and holding distribution rights for the program data based on a contract with said manager, for encrypting program data by the encryption key issued from the manager and distributing the encrypted program data along with the corresponding identification code; a key server, connected to said open network, and independent from the file server, for distributing the decryption key issued by said manager; and a terminal, connected to said open network, for receiving the encrypted program data along with the corresponding identification code from the file server, and obtaining the decryption key corresponding to the identification code from the key server to decode and process the encrypted program data.

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)